Advanced Malware **Exposed**

How advanced malware, zero-day and targeted APT attacks are evading today's network defenses

Foreword by Robert Lentz
Former CISO, Department of Defense

Table of Contents

Chapter 1: Why Today's Network Defenses Fail 4

Chapter 2: Firewalls, IPS, Antivirus, and Web Gateways: Fighting Yesterday's Threats 9

Chapter 3: Understanding Advanced Malware 16

Chapter 4: The "Operation Aurora" Incident: A Case Study in Security Failure 20

Chapter 5: What Happens Next? 23

Foreword

In the last ten years, malicious software—malware—has become increasingly sophisticated, both in terms of how it is used and what it can do. This rapid evolution of malware is essentially a cyber "arms race" run by organizations with geopolitical agendas and profit motives. The resulting losses for victims have run to billions of dollars. The global move to digitize personal and sensitive information as well as to computerize and interconnect critical infrastructure has far outpaced the capabilities of the security measures that have been put into place. As a result, cyber criminals can act with near impunity as they break into networks to steal data and hijack resources. It is difficult to stop their criminal malware and nearly impossible to track them down after an attack has been perpetrated.

This handbook shines a light on the dark corners of advanced malware, both to educate as well as to spark renewed efforts against these stealthy and persistent threats. By understanding the tools being used by criminals, we can better defend our nations, our critical infrastructures and our citizens. The "Operation Aurora" incident represents an example of how the threats have escalated, revealing how advanced malware is being used in a systematic, coordinated fashion to achieve nation-state objectives. Meanwhile, organized crime's use of malware has already created a multi-billion dollar industry in which identities, computing resources, and intellectual property are stolen and traded to the highest bidder.

We must protect against the cyber attacks of those seeking to steal, compromise, alter or destroy sensitive information. It is clear that organizations must better integrate information security into enterprise architectures to protect data as well as to unify operations. Integrated, enterprise-wide, risk-based protection strategies should enable the agile deployment of innovative security technologies. A range of companies, including those within the financial services, healthcare, energy, and the Defense Industrial Base (DIB) sectors, deserve and should demand security technologies that can adapt to ever-evolving malware and form the basis of a more resilient, penetration-resistant information system.

The Internet has spawned entirely new ways of doing business, both legitimate and illegal, and this story is only beginning. The steady stream of news about data breaches and lost identities will only be the tip of the iceberg—unless we invest the time, money and effort to re-think IT security. In the battle against a well-funded, sophisticated adversary, IT security professionals continue to lead the way. With education and investment, we can cut the puppet strings being used to seize control of our networks. It is certainly my hope that this book will provide readers with a new understanding of the rapidly developing cyber threat landscape and practical insights into how they can protect their data and computing infrastructures.

> *"By understanding the tools being used by criminals, we can better defend our nations, our critical infrastructures and our citizens. The "Operation Aurora" incident represents an example of how the threats have escalated, revealing how advanced malware is now being used in a systematic, coordinated fashion to achieve nation-state objectives.*

— Robert F. Lentz

President and CEO, Cyber Security Strategies, LLC; Former CISO for the DoD; and the first DoD Official to serve as Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance

Chapter 1: Why Today's Network Defenses Fail

Look at any technology news site, and you will see regular stories about successful attacks and the continued discovery of new vulnerabilities. Here is a collection of headlines from one site[1] on an average day, April 26, 2011:

"FBI warns of millions lost in fraudulent transfers to China"

"PlayStation Network hacked, data on millions at risk"

"Department of Energy-funded lab silenced by APT attack"

"Stars" worm targets systems in Iran, official says"

"New report finds most applications don't pass security tests"

Industry analysts estimate that, on any given day, anywhere from 5% to 10% of all PCs are infected with sophisticated, remotely controlled malware.[2] This translates to 50 to 100 million compromised PCs worldwide. One thing is clear: today's network security defenses are not working against today's malware. The chart on the following page plots the effectiveness of current defenses in guarding against malware.

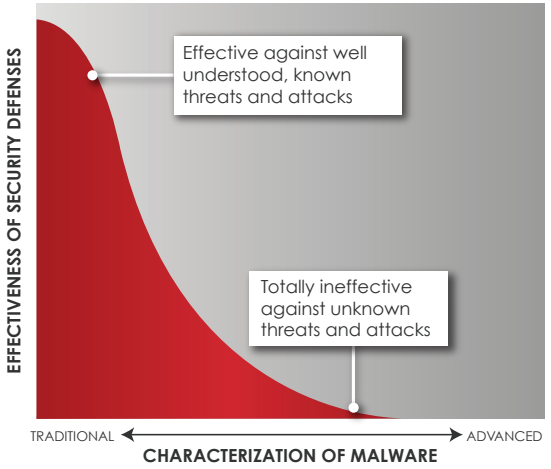
What we see is that today's network defenses are aggressively evaded by malware that is even moderately advanced. Why is this? In order to answer this question, we first have to define advanced malware. The table on the following page describes four key characteristics to explore in classifying malware.

---

[1] http://www.scmagazineus.com/ as of April 26, 2011
[2] http://arstechnica.com/old/content/2007/01/8707.ars

Traditional Defenses (NGFW, IPS, AV, SWG)
Inability to Combat Advanced Malware

Effectivity vs. Advanced Malware



Characterizing Malware

Stealth level	Ranges from high to low. Does the malware actively hide or cloak itself using techniques like polymorphism or code obfuscation?
Targeted vulnerability	Malware can target known, unpatched vulnerabilities as well as unknown vulnerabilities, known as “zero-day” attacks, in plug-ins, browsers, applications or the OS.
Intended victim(s)	Malware can attack indiscriminately, or it can target specific victims using spearphishing emails and compromised websites.
Objectives	Malware can be used to cause disruption or as a tool for organized theft and cyber crime.

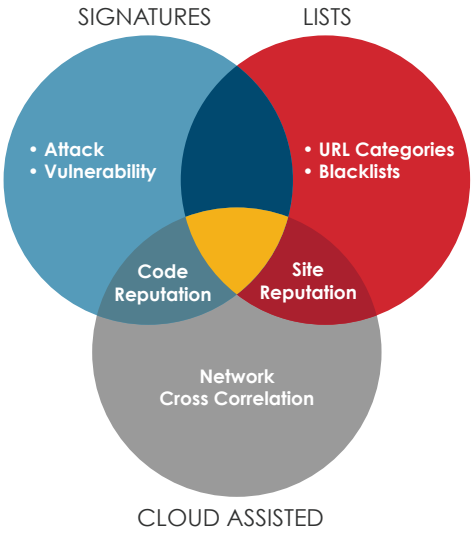
Based on these characteristics, we can now profile specific malware. The following chart illustrates the characteristics that separate today's advanced malware from conventional malware.

If we look at an example like Operation Aurora, we see stealthy malware attacking a previously unknown vulnerability in Internet Explorer. Further, the criminals behind Aurora targeted a well-defined set of organizations and had a clear goal: the theft of email archives and other information. When it comes to the definitions of advanced malware, Aurora clearly meets all the criteria. The scary part is that Aurora is not the most advanced example of today's malware. Stuxnet and Zeus showcase the continued refinement of malware tactics, leveraging multiple zero-day vulnerabilities and evolving over time. The Epsilon marketing theft showed a shift to procuring email addresses to enable targeted phishing, or spear phishing campaigns. The headlines mentioned earlier—millions of

accounts lost, national labs targeted—foreshadow other attacks that will become iconic in our industry.

Why do today's defenses fail when confronted with advanced malware, zero-day, and targeted APT attacks? For many organizations, IT security is made up of layers of firewalls, intrusion prevention systems (IPS) and antivirus software, deployed both in network gateways and desktops. Today, there are many variations of these technologies, including cloud-based alternatives. These solutions are built on two fundamental protection technologies: lists and signatures. The following chart depicts the categories and interrelationships of today's malware defense alternatives.

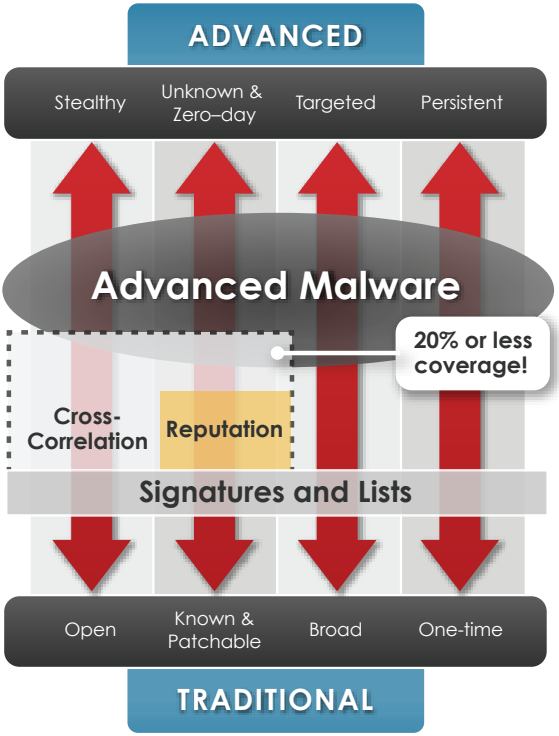
Network Malware Protection Techniques



It is by comparing the malware characteristics and the available malware defense mechanisms that the shortcomings become clear. As shown in the chart on the next page, advanced malware operates at the top of the malware chart, while the current generation of network defenses operates at the bottom. For example, signature-based mechanisms react to known attacks

and fail against unknown and stealthy attacks. Further, reputation, heuristics, and other correlating techniques cannot guard against targeted attacks, because, given the nature of these attacks, there is no existing data to correlate.

Conventional Defenses Don't Address Advanced Malware



Quite simply, we are using outdated, conventional defenses to guard against cutting-edge, innovative malware. We are no more prepared to do this than a 19th century army trying to defend itself against today's electronic weaponry. We must find defense mechanisms that address the characteristics of both advanced and conventional malware.

Chapter 2: Firewalls, IPS, Antivirus, and Web Gateways: Fighting Yesterday's Threats

The evolution of modern society's dependency on technology is being fueled both by technological advances and by our desire for the convenience offered by digitizing our social and business interactions.

Our yearning for openness and ease of access comes with a price, however. The very thing we are striving for, having the world at our fingertips, is also what has driven the exponential increase in cyber crime. With each new advance, criminals and rogue nation states gain another opportunity to steal, manipulate, disrupt and destroy.

In its effort to thwart these attacks, the security industry has delivered a range of technologies. While many of these technologies were of limited benefit and quickly shelved, others have become the de facto standards for many organizations, seen as essential in adequate security.

Today, four technologies function as the main pillars of most organizations' security frameworks: firewalls, intrusion prevention products, antivirus software and Web gateways. While technologies like firewalls and antivirus undoubtedly remain essential to sustaining some level of security, it is also equally unmistakable that these technologies, even when combined, are not enough to prevent today's advanced malware attacks. Even next-generation firewalls fall short, since they are optimized to enforce policies on users and applications and consolidate traditional technologies, rather than detect and block fast-changing threats.

In order to understand the current security gap, it is important to examine why these security products were created, and where they have limitations. By assessing these limitations, we can see why these technologies alone are no longer enough, and why the threat protection paradigm must now shift to counter the way threats have shifted.

Firewalls

When network-based communications and services were in their infancy, the biggest threat was from outside attackers seeking to probe and compromise internal systems. In order to limit who was allowed to communicate with systems on a corporate network, the firewall was born.

The purpose of firewalls, then and now, is to give organizations the ability to strictly limit which systems can communicate with internal systems, and which ports can be used for those communications. Firewalls thus shield systems and services that should not be generally accessible and that would otherwise be vulnerable.

While attacks used to be more specific to servers and network-based vulnerabilities, the threat landscape has changed. Today, both the initial attacks that compromise computer systems and subsequent malware communications tunnel over protocols such as HTTP, which corporations must allow through the firewall. Traditional firewalls can only limit which systems can communicate through particular ports or protocols, but they were not designed to inspect the communications themselves.

Thus, while they are a necessity for organizations, firewalls are completely blind when it comes to preventing any of today's targeted and zero-day malware attacks.

Next-generation firewalls are enhanced to impose policies based on users and applications, so they work for compliance, but not for detecting breaking threats. Next-generation firewalls also bundle in some signature-based technologies like anti-virus and intrusion detection. However, they do not offer new threat detection or protection capabilities. At a practical level, these firewalls often have their CPUs full applying rules and don't have cycles left for thorough inspection for emerging and unknown threats. With some vendors, it is common for security options to be turned off to prevent introducing latency into the network. So you pay for protection you don't use, then pay to clean up the problem.

Network Intrusion Prevention

Network intrusion prevention systems (IPS), and the intrusion detection systems (IDS) that preceded them, were developed to address the firewall's visibility and granularity limitations. To filter out attacks, IPS solutions inspect network communications to understand the various application data being transmitted.

Earlier IDS solutions performed passive monitoring, analyzing network traffic and identifying the attack based on signatures of known exploits. As IDS morphed into IPS, these solutions could prevent attacks in which a signature had matched a known exploit.

Over time, IPS vendors began to claim that their solutions could prevent unknown, or zero-day attacks. In reality, however, these claims have not proven to be true. These claims were based on the shift from IDS detection of an individual attack based on an exploit signature to IPS detection of a class of attacks based on a vulnerability signature. This basic improvement provided the basis for vendors' zero-day protection claims, specifically that attacks against a particular vulnerability would be stopped whether a known or unknown exploit was being used. The critical part IPS vendors fail to mention is that this unknown exploit prevention is based on having a rich understanding of the vulnerability universe. In other words, IPS vendors have moved the network signature problem from one of having to know about all exploits to that of having to know about all vulnerabilities.

The challenge is that vendors must account for both the exponentially increasing number of known vulnerabilities, as well as all the unknown vulnerabilities in today's threat landscape. It simply proves to be impossible given how IPS technology was originally designed. So today, we find that the most severe and successful attacks against organizations are those that exploit unknown vulnerabilities. It is only after these attacks eventually become public, thus prompting a vulnerability disclosure, that IPS vendors are able to reactively update their products to look for exploits targeting these previously unknown vulnerabilities.

The other major limitation of IPS offerings is that these systems were originally built to detect and analyze network services-based attacks on the OS and server applications, rather than the client-side application attacks that dominate the landscape today. The everyday client applications being used by consumers and business users, such as browsers, PDF readers and Flash plug-ins, are the number one target for attackers. The ability for attackers to encapsulate and obfuscate these application-based attacks within layer upon layer of application and network protocols makes it nearly impossible for IPS systems to find the needle in the haystack. Not to mention, even if they could identify these attacks, it is only for attacks against known vulnerabilities, while most attacks target the unknown.

Antivirus

In order to counteract the limitations of firewalls and IPS, many companies run antivirus software on every individual computer system. Similar to older IDS products, antivirus software maintains very large databases of known threats. Should the signature of a threat be identified on a system file, that file can then be quarantined or removed.

Here again, security teams are using a reactive solution, one that requires them to rely on security vendors to know about threats in advance in order to prevent them. As advanced malware and other threats increasingly focus on the unknown and grow more dynamic, antivirus is left completely helpless in combating today's attacks.

Web Gateways

By now, you might be noticing a pattern: What the traditional security industry refers to as "defense-in-depth" has so far been iterations of pattern-matching techniques deployed in network or host-based systems. These technologies represent an ongoing effort to augment basic port-based blocking and to overcome the inherent limitations

of the previous round of signature-based or list-based security product deployments. Web gateway security is no different.

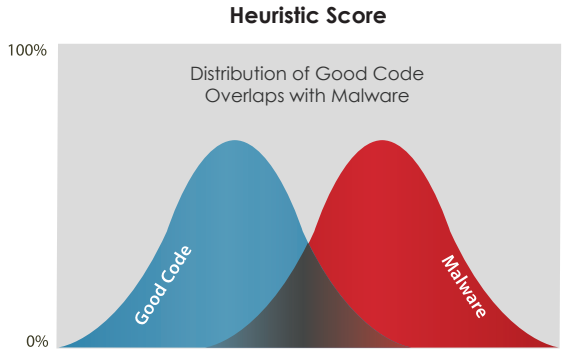
As attackers shifted tactics to deliver both attacks and malware communication over the Web, organizations found a need to tighten their control over Web-based communications. As a result, Web gateways were developed. These technologies, like the ones before them, use lists of "known bad" URLs and do not look to the evolving, unknown threats of the future. Vendors have based their prevention capabilities on a list-based approach, preventing the transmissions of Web data and Web sites that were known to be malicious.

While Web gateways provided some initial security value, attackers have shifted tactics. They have moved to completely dynamic and obfuscated models of both attack delivery and malware communication, which render lists of malicious Web sites obsolete. Consequently, just as Web gateways were beginning to be widely adopted, they became outmoded from a security perspective. While these technologies still have utility in enforcing HR policies that limit employee Web browsing, when it comes to combating modern attacks, Web gateways have been relegated to an increasingly marginal security role. The same is true of antivirus and other technologies due to the shift in tactics by cyber criminals.

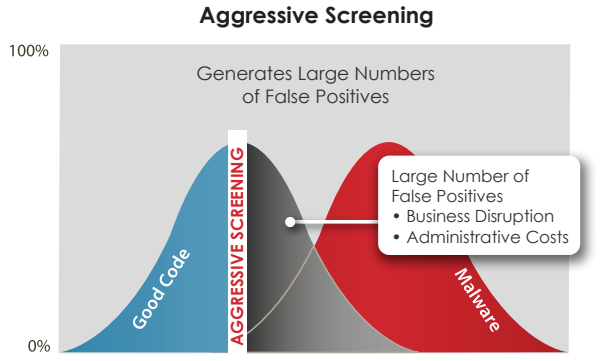
The Dilemma of Heuristics

Some vendors have tried to close the coverage gap outlined above by layering on heuristics-based filtering. Heuristics are essentially "educated guesses" based on behaviors or statistical correlations. They require fine-tuning to account for specific circumstances and to reduce error rates (or to increase confidence levels, statistically speaking.) While this technique is a step in the right direction, it is not enough by itself, or even when layered with signature-based or list-based techniques. Because advanced malware shares some characteristics common to all modern

software, heuristic developers are faced with a fundamental trade-off. To trigger on (or positively identify) the growing types of malware code, developers create broader sets of heuristics that will, by definition, increasingly encompass benign "good" software code. The following chart illustrates the challenge.



If an aggressive heuristic detection policy is implemented, it will generate a huge number of false positives, as illustrated below. This is unworkable because these false alerts disrupt business and create huge challenges for administrators, who must sort through massive volumes of false positives to identify the true positives. On the other hand, it is easy to see how a less aggressive heuristic detection would reduce false positives, but would then increase the number of missed malware incidents. This is ultimately a tenuous trade-off: opting for usability at the price of lowering security.



The Limitations of Backward-Looking Techniques

In reviewing the evolution of traditional security technologies, it is easy to grow disheartened by the challenges of securing an organization's sensitive information. The reality, though, is that the security landscape does not need to be one of doom and gloom.

A look at the limitations of prior security technologies reveals a common theme: these prior approaches all attempt to itemize known exploits and vulnerabilities into lists or signatures. That common approach has also led to their collective collapse underneath the avalanche of vulnerabilities and exploit techniques. It is clear that the threat landscape will continue to change at a rapid pace, in ways we cannot dream of, just as we cannot dream of all the ways technology will be used in the future. The one thing that remains constant in every attack, however, is the end result of a compromise and the end game of attackers: data theft and disruption.

To create a lasting security technology, one that can dynamically and proactively shift to stay ahead of evolving threats, security teams will need solutions that do more than rely on URL lists and signatures of known exploits and disclosed vulnerabilities. Instead, they will need technologies that can accurately identify attacks against previously undisclosed vulnerabilities, exploits and techniques in real time. They would then be able to apply these findings to prevent system compromise and data theft.

> *"The highest technique is to have no technique. My technique is a result of your technique; my movement is a result of your movement."*
>
> *– Bruce Lee*

Chapter 3: Understanding Advanced Malware

The modernization of malware has been characterized by attackers' quests to gain increasing control of compromised computer systems. Whether attackers use viruses, Trojans, spyware, rootkits, spear phishing, malicious email attachments or drive-by downloads; their malware enables the simple disruption or long-term control of compromised machines.

There is a dramatic difference between the earliest forms of malware and the malware we are faced with today. When computer security was in its infancy, attackers were typically compromising systems for fame or bragging rights. To that end, the first types of malware came in the forms of computer viruses that could spread across multiple machines, with a goal of causing some notoriety for the virus author. Later iterations of viruses came in the form of the worm. Worms leveraged software vulnerabilities to spread across multiple computers in completely automated fashion, rather than the social engineering required by earlier viruses.

While some computer worms ended up having serious and negative side effects, the vast majority was written for notoriety. Because these early types of malware were more about fame, they also tended to be "noisier" and easier to detect with common signature-based approaches. In some cases, worms were intended as initial exploratory attacks to set the stage for future, more aggressive attacks, as is believed to be the case with CodeRed. As criminals became aware of the value of information being placed online, they quickly got involved in the development, sale and purchase of malware. It is clear that criminals with profit motives or political agendas are the main cause for the explosion of advanced malware as we know it.

These criminals are concerned not with fame but with fortune, driven not by ego but by gain. The advanced malware these criminals have developed is persistent, stealthy and dynamic and leverages unknown attack vectors. The specific characteristics

differ depending on the motives of the attackers, with malware being used for cyber crime, cyber espionage, and emerging cyber warfare scenarios.

Cyber Crime

When it comes to cyber crime, the criminal's main goal tends to center on stealing financial information that can eventually be turned into hard currency. There are indirect ways these attackers are making money, often by setting up compromised networks of computers that are used for performing spam and distributed denial of service attacks. These massive arrays of computers, called "botnets," are then monetized in a variety of ways. For example, some criminal organizations rent out the computing power of these networks to businesses marketing their products via spam. In other cases, criminals perpetrate extortion schemes by threatening to take a company's website down through distributed denial of service attacks.

Increasingly, cyber criminals are focused on stealing financial and personal information that can be more easily monetized, leveraging phishing emails targeted with data available on the Internet.

> *"Customers of a telecommunications firm received an email recently explaining a problem with their latest order. They were asked to go to the company website, via a link in the email, to provide personal information—like their birthdates and Social Security numbers. But both the email and the website were bogus."*
>
> *— www.FBI.gov*[3]

[3] SOURCE: http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

Spear phishing uses personalization and research to catch a more valuable prize, like logins for corporate bank accounts and corporate applications, which can lead to theft of intellectual property. Instead of blasting out millions of emails and counting on a few victims to bite, spear phishers target select groups or companies with something in common: they work in the same industry, do business with the same financial institutions, or are alumni of the same college. The emails are sent from trusted organizations or individuals from whom the potential spear phishing targets would regularly get emails, making them even more deceptive.

Spear phishing messages often lure privileged users to click on a URL to a site where malicious code can be downloaded, or ask users to a plausible-looking attachment that contains dropper malware (code that can dial out to the criminal's server to collect malware) or a keylogger. A recent phishing attack distributed a malicious file named: *Disentangling Industrial Policy and Competition Policy.doc*.[4]

In response, financial institutions have added increased layers of security around authentication and identity verification, including two-factor authentication and cell phone or SMS pin code authorizations for bank transactions. Virtually overnight, however, malware has evolved to circumvent these new safeguards. Zeus is one example of clever malware that leverages SMS authentication to achieve success.

Cyber Espionage

The level of sophistication and focus characterized by cyber crime is also evidenced by cyber espionage. Cyber espionage is a term that should not be used lightly. No longer a vehicle for Hollywood B-movies that mix hacking and spying, cyber espionage is a very real threat today. One of the central themes of espionage has always been developing assets with access to information. Now, the assets with

[4] http://www.virustotal.com/file-scan/report.html?id=1e677420d7a8160c92b2f44f1ef5eea1cf9b0b1a25353db7d3142b268893507f-1302359653

access to the information are not only human assets, but also computer-based assets. As more information is digitized and put online, we will only see an increase in the use and sophistication of cyber espionage.

Given the relatively low barriers to entry, superior cyber espionage capabilities will not be the exclusive domain of traditional super powers. No doubt, the efforts of much of the global intelligence community focus on cyber espionage. There have been a few public cases of advanced malware being used in corporate espionage, including Operation Aurora and an attack targeting the oil industry.

In both cases, malware that was stealthy and unknown to signature-based systems was highly effective in stealing sensitive information. More worrisome than the low cost of entry into cyber espionage is the problem of attribution. We have seen in both attacks that data eventually made its way back to servers in China. Given the networked nature of computers and the ability to cover your tracks in cyber space, it is very difficult to prove the attacker's origin or identity and respond accordingly. As societies grow increasingly reliant upon technology, these challenges will only grow more daunting.

Cyber War

We have yet to really experience what full-scale cyber war will look and feel like. We know that sophisticated technical capabilities, including hacking, have had limited usage within conventional warfare scenarios thus far, but we have yet to see a coordinated and targeted attack against a country's information and infrastructure. Make no mistake, the reason we have not seen such an attack is not necessarily because of the lack of technical capabilities, but more likely because no one has pulled the trigger—yet. We can only hope that by the time any coordinated cyber attack on infrastructure takes place that we have progressed past politics and what-if scenarios and begun to take corrective action. As with espionage, it is only a matter of time before enemies target the critical infrastructure we are ever increasingly reliant upon, and upon which so much of our way of life is based.

Chapter 4: The "Operation Aurora" Incident: A Case Study in Security Failure

On January 12th 2010, Google honorably disclosed to the world that it had been a victim of an advanced persistent threat (APT) attack. It was soon discovered that Google was one of more than 20 companies successfully targeted by a well-organized and coordinated effort to gain access to sensitive systems and information. Victims ranged across industries, including the financial, technology and chemical sectors. These attacks later became known as "Operation Aurora" and are a very useful example of what modern attacks with malware actually look like—and how commonly used security technologies completely fail in combating these attacks.

The attacks started in December 2009, leveraging an unknown (zero-day) Internet Explorer 6.0 vulnerability. Once a system was compromised, the attackers installed a Trojan. This Trojan malware would then communicate back to a criminal command and control server that had the ability to issue a variety of different commands, enabling attackers to gain additional access within compromised companies' networks and systems.

The first stage of the Aurora attack was to lure users into clicking on a website link that would direct the user's Web browser to the attacker's Web server. This activity was not identified as suspicious by firewalls, IPS, antivirus, or Web gateways; it is behavior that happens constantly during the normal course of Web browsing. Once a victim's Web browser loaded the malicious website, an unknown vulnerability within Internet Explorer was exploited in order to run malicious code. As it targeted an unknown vulnerability, IPS products were not preventing this exploit, so these devices had no generic vulnerability signature. Likewise, because this attack was coming from a website that was not yet in any malicious website database, Web gateway technologies were not able to filter out these Web requests.

Once the Internet Explorer exploit was successful, the second stage was to download a Trojan that would give attackers the access they needed to manipulate compromised systems. This malware was custom developed and therefore not yet known to the antivirus industry, so a signature had yet to be manually created. As a result, desktop antivirus software was just as blind to the attack as firewalls and IPS. Antivirus companies later released signature detection updates, once the attacks had long passed, and called the Trojan component "Hydraq."

The 20 companies victimized by Operation Aurora relied upon a range of common security technologies. At all levels, the technologies that these companies were relying upon failed them.

The antivirus industry was especially quick to tell the world that the exploit and malware was the most technically sophisticated attack they had ever seen. The coordination and logistics of targeting more than 20 companies successfully in a very short period is no doubt a testament to the high level of sophistication of the attackers.

However, what is important to understand is that Aurora used fairly conventional malware—the specific vulnerability, exploit and malware were no more sophisticated than those of many other recent malware attacks—in unconventional ways.

In fact, Operation Aurora's Trojan, its communication capabilities and resiliency were less sophisticated than those of many massively deployed botnets. By using several stages, inbound and outbound communications over different protocols, and zero-day techniques, what Aurora did was bypass each layer of security. No individual layer inspected across vectors and stages to witness the entire attack.

The bottom line is that antivirus, as well as IPS and other traditional security mechanisms, failed to provide organizations with the

necessary level of protection. These attacks clearly illustrate the shortcomings of today's common security technologies in safeguarding against attacks that leverage unknown, therefore unpatchable, software vulnerabilities along with custom malware. Quite simply, reactive, signature-based approaches are unable to solve this dynamic and polymorphic problem.

The effects of these attacks were not felt just by the 20 plus organizations originally targeted. As soon as details emerged on the Aurora attacks, more information surfaced about the unpatched Internet Explorer vulnerability. Consequently, unrelated malicious websites were soon popping up en masse to victimize any unsuspecting Internet user who had an older version of Internet Explorer and visited the wrong website at the wrong time. In these cases, unrelated cyber criminals exploited this vulnerability, like so many others, to enslave computer systems to massive bot networks that could subsequently be used for information theft, DDoS attacks and spam generation.

This later stage shows how zero-day attacks that target large enterprises have an eventual trickle down effect to both smaller businesses and consumers alike. Since the Internet Explorer zero-day vulnerability was still not yet well understood by an industry built on reactive signatures, the smaller businesses and consumers were offered no protection until much later. Without a doubt, this cycle must end and end quickly—the stakes of technology compromise only grow with each passing day.

Chapter 5: What Happens Next?

Today's malware is not yesterday's virus. The anachronistic concept of protecting information with an outdated technique like signatures has left many businesses, government organizations and consumers vulnerable to attack. Signature-based technologies like IPS and antivirus software, both within perimeter and endpoint solutions, are ineffective against the rapidly evolving, blended threat of advanced malware. To be effective, anti-malware solutions need to be intelligent enough to analyze network traffic and processes, rather than just comparing bits of code to signatures or lists.

Heuristic, or behavioral, analyses are an encouraging development, but too inaccurate to function as standalone security mechanisms. This methodology augments an anti-malware solution's signature protections, but at the same time increases the likelihood of false positive alerts.

Modern threats are made up of attacks on multiple fronts, exploiting the inability of conventional network protection mechanisms to provide a unified defense. As soon as one vulnerability is defended, network attacks quickly shift to another.

The sheer volume and escalating danger of modern attacks are overwhelming limited IT resources and outmaneuvering conventional defenses. For most enterprises, conventional network connection-oriented and software-based defenses are inadequate because of the gaps they leave in security coverage, but trying to integrate conventional defenses from multiple vendors is far too complicated and costly an undertaking for an enterprise IT group.

The only viable solutions are those that provide thorough coverage across the many vectors that are used in attacks and that can keep

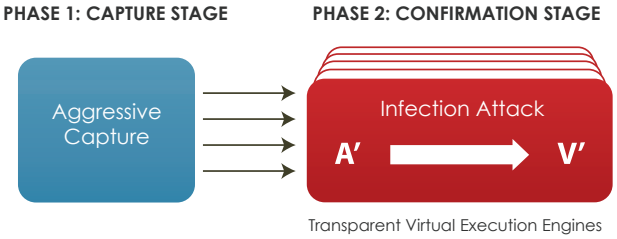
pace with the dynamic nature of targeted APT attacks. Defending corporate networks from advanced malware threats requires new protections that function across many protocols and throughout the protocol stack, including the network layer, operating systems and applications.

In order to address these tailored and sophisticated threats, a real-time, dynamic and accurate analysis capability is critical. Rather than relying on signatures and lists, we must be able to dynamically learn new vulnerabilities, exploits and techniques in real time, and then prevent system compromise and data theft.

Next-generation Threat Protection from FireEye

To meet these requirements, FireEye has developed advanced malware protection that delivers accurate analysis for zero-day, targeted attacks—without relying on signatures. Without prior knowledge of exploits or browser-, application- or OS-level vulnerabilities, it identifies targeted, stealthy malware using a multi-phase analysis engine. In addition, the FireEye solution provides deep packet inspection of outbound communications across multiple protocols to identify and block infected systems that attempt to communicate with criminal servers.

We provide real-time, dynamic protections against zero-day, targeted and APT malware through a multi-stage inspection engine that combines heuristic analyses with deep packet inspection within instrumented virtual machines. Phase 1 is a set of aggressive capture heuristics used to identify suspicious network activities. As we stated previously, aggressive heuristics used in isolation will generate a high rate of false positives. However, output from FireEye's phase 1 flows into phase 2, the confirmation stage. In phase 2, network traffic flows are replayed into virtual execution engines to validate if the traffic is indeed attack exploit code.



These virtual execution engines act as a Petri dish of sorts, confirming whether or not suspicious code actually infects a system while also eliminating false positives. Now, aggressive heuristic policies can be set to flag even mildly suspicious network traffic with the understanding that the subsequent malware analysis stage would confirm the actual attack traffic as well as eliminate any false positives. By combining a system that minimizes missed attacks with a system that eliminates false positives, we can approach our ideal analysis engine, namely one which does not miss zero-day attacks nor produce false alerts. This multi-stage analysis also enables the programmatic capture, fingerprinting and blocking of zero-day malware and its unauthorized outbound callbacks to criminal command and control servers.

Global Sharing of Local Malware Intelligence

In order to share the benefits of the real-time malware intelligence gathered by the local analysis engines, we have built a worldwide network to distribute the auto-generated security intelligence about confirmed malware and its covert callback channels. As new organizations opt in to our Internet cyber crime watch, the latest intelligence on inbound attacks and unauthorized outbound communications is shared in real time to prevent data exfiltration, alteration and destruction.

FireEye makes it possible to combat advanced malware, zero-day and targeted APT attacks in real time. With inbound attack detection and outbound malware transmission filtering as well as

a global malware protection network in the cloud, administrators have a clientless solution that is easy to deploy and maintain to provide advanced protection against today's threats.

It is more important than ever to secure our infrastructures from cyber criminals as our everyday activities increasingly rely on a safe and stable network. FireEye intends to continue to equip security leaders with next-generation protection so that the next few chapters of the advanced malware story will reflect organizations regaining control of their network resources, sensitive data, and computing assets.

About FireEye

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as next generation and traditional Firewalls, IPS, AV and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.

FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035

+1 (877) FIREEYE (347.3393)
info@fireeye.com